IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Mohamed Khlil et al.	§	Attorney Docket No. 11349RRUS04U / 22171.321
Serial No. 10/089,752	§	Customer No. 27683
Filed: June 24, 2002	§	Group Art Unit: 2134
For: KEY EXCHANGE FOR NETWORK ARCHITECTURE	§	Examiner: Ellen C. Tran
	§	Conf. No.: 2811

Mail Stop Appeal Brief - Patents
Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL

The following Appeal Brief, with Appendixes, is being submitted for the above-identified patent application. The Commissioner is hereby authorized to charge the fee of $500 for filing the Appeal Brief and any other fees associated with these papers or their enclosures, or to credit any overpayment, to Deposit Account No. 08-1394 of Haynes and Boone, LLP.

Respectfully submitted,

David M. O'Dell
Registration No. 42,044
(972) 739-8635

Date: March 29, 2007

HAYNES AND BOONE, LLP
901 Main Street, Suite 3100
Dallas, Texas 75202-3789
Telephone: 972-739-6900
Facsimile: 214-200-0853
File: 11349RRUS04U / 22171.321

R-162653.1

Certificate of Service

I hereby certify that this correspondence is being filed with the U.S. Patent and Trademark Office via EFS-Web on 3-29-07.

Bonnie Boyle
Bonnie Boyle

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Mohamed Khlil et al.	§	Attorney Docket No.: 11349RRUS04U / 22171.321
	§	
	§	Customer No. 27683
Serial No.: 10/089,752	§	
	§	Group Art Unit: 2134
Filed: June 24, 2002	§	
	§	Examiner: Ellen C. Tran
For: KEY EXCHANGE FOR NETWORK ARCHITECTURE	§	Confirmation No.: 2811
	§	

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

APPEAL BRIEF

A timely Notice of Appeal was previously filed on January 29, 2007, in order to initiate an appeal from the action of the Primary Examiner in finally rejecting all of the pending claims (Claims 16-30 and 70-75) in an Office Action mailed on October 27, 2006. This Appeal Brief is being filed pursuant to the provisions of 37 C.F.R. §41.37. A separate transmittal letter containing an appropriate certificate of service serves to transmit (1) this Appeal and (2) the fee of $500 under 37 C.F.R. §41.37(a)(2) and §41.20(b)(2) for filing this Appeal Brief.

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The real party in interest is NORTEL NETWORKS LIMITED, a Canadian company having a principle place of business at 2351 Boulevard Alfred-Nobel, St. Laurent, Quebec H4S 2A9, Canada.

RELATED APPEALS AND INTERFERENCES

There are no prior or pending appeals, interferences or judicial proceedings known to appellant, appellant's legal representative, or the assignee that may be related to, directly affect, be directly affected by or have a bearing on the Board's decision in the present appeal.

STATUS OF CLAIMS

Claims 1-15, 31-69, and 76-127 have been canceled. Claims 16-30 and 70-75 are all pending, have all been finally rejected, and are all on appeal here.

STATUS OF AMENDMENTS

No amendment or response has been filed since mailing of the final rejection on October 27, 2006.

SUMMARY OF CLAIMED SUBJECT MATTER

To clarify the summary of the claimed subject matter, at least some representative portions of the specification and drawings related to the recited claim elements are set forth parenthetically below. However, there may be further portions of the specification and/or drawings that are also relevant to the claimed subject matter.

The subject matter recited in independent Claim 16 of the present application relates to a method of providing secure communication (Fig. 2, reference nos. 112, 114) between a mobile node (Fig. 2, reference no. 102) and home domain (Fig. 2, reference no. 108) using a foreign domain (Fig. 2, reference no. 106), comprising:

transmitting a registration request (Fig. 5, reference no. 300; page 12, lines 18-22) from the mobile node to the home domain (Figs. 3a & 3b, reference nos. 210, 212, 214; page 12, line 15 through pg. 13, line 4) the request comprising an identity of a user of the mobile node in encrypted form (Fig. 5, reference nos. 304, 306; page 12, lines 22-31) and network routing information in non-encrypted form (Fig. 5, reference no. 302; page 12, lines 18-31);

the home domain receiving and processing the registration request (Fig. 3b, reference nos. 218, 220 ; page 13, lines 11-19) to generate a registration reply (Fig. 6, reference no. 400; page 13, lines 20-30) comprising one or more encryption keys (Fig. 6, reference nos. 404, 406, 408, 410; page 13, lines 16-30) for encrypting messages communicated between and among the mobile node, home domain, and the foreign domain (Fig. 7, reference no. 500; page 14, lines 12-21); and

transmitting the registration reply from the home domain to the foreign domain and the mobile node (Fig. 3b, reference no. 224; page 13, lines 20-30).

The subject matter recited in independent Claim 70 of the present application relates to a method of providing secure communications between an initiator (Fig. 25, reference no. 13002) and a responder (Fig. 25, reference no. 13004) in a communication network, comprising:

dynamically establishing a security association between the initiator and the responder (Fig. 25, reference nos. 13002, 13004; page 25, lines 6-14), whereby the initiator presents to the responder a registration request (Figs. 25 & 26, reference no. 5000; page 25, lines 6-23) that includes one or more proposals (Fig. 26, reference no. 6004; page 25, line 6 through page 26, line 2).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether Claims 16-30 are unpatentable under 35 U.S.C. §103 as obvious in view of a proposed combination of Inoue et al. U.S. Patent No. 6,501,767 (hereinafter referred to as "Inoue") and Tisdale et al. U.S. Patent No. 5,708,716 (hereinafter referred to as "Tisdale").

2. Whether Claims 70-75 are unpatentable under 35 U.S.C. §103 as obvious in view of a proposed combination of Chuah et al. U.S. Patent No. 6,400,722 (hereinafter referred to as "Chuah") and Cheng et al. U.S. Patent No. 6,418,130 (hereinafter referred to as "Cheng").

ARGUMENT

I. THE §103 REJECTIONS OF CLAIMS 16-30

Claims 16-30 stand rejected under 35 U.S.C. §103 as obvious in view of a proposed combination of Inoue and Tisdale. However, it is respectfully submitted that Claims 16-30 are not obvious in view of Inoue and Tisdale. In this regard, the PTO recognizes in MPEP §2142 that:

> The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness.

Applicants respectfully submit that Inoue and Tisdale fail to establish a *prima facie* case of obviousness under §103 with respect to Claims 16-30, for mutually exclusive reasons that are discussed below.

The Prior Art Must Teach All Claim Limitations Under §103

As discussed in MPEP §2142, case law relating to §103 requires that:

> To establish a *prima facie* case of obviousness . . . the prior art reference (or references when combined) must teach or suggest **all** the claim limitations. . . . *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). (Emphasis added).

Applicants' Claim 16 includes a recitation of:

> . . . the home domain receiving and processing the registration request to generate a registration reply comprising one or more encryption keys for encrypting messages communicated between and among the mobile node, home domain, and the foreign domain; . . . .

Applicants respectfully submit that neither Inoue nor Tisdale, alone or in combination, teach or suggest all the features of Claim 16. The Examiner indicated that "the following is not taught in [Inoue]: 'comprising one or more encryption keys for encrypting messages to be communicated between and among the mobile node[,] home [domain, and the foreign domain].'" (See Final Office Action, pg. 8). The Examiner goes on and alleges that Tisdale cures the deficiencies of Inoue by teaching such features in Col. 7, line 63 through Col. 8, line 3. (See Final Office Action, pg. 8). Applicants respectfully disagree. More specifically, the cited passage of Tisdale recites the following:

> ...It is another feature and advantage of the satellite communication system to provide a fraud detection and user validation system where keys are not transmitted "over the air" in the clear. It is another feature and advantage of the satellite communication system to provide a fraud detection and user validation system where the keys are changeable at the MET, and a simple one-time entry/validation system.

The Examiner further alleges that "[i]t would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of [Inoue] a mobile communication scheme to include means to generate a reply that utilizes one or more encryption keys as taught in [Tisdale]." (See Final Office Action, pg. 8). From the above, Tisdale only generally describes a

fraud detection and user validation system using security keys. As such, Tisdale uses security keys for validation to prevent unauthorized access by a MET (Mobile Earth Terminal) to a communication system. Nowhere in the cited passage does Tisdale teach or suggest, a registration reply that "comprises one or more encryption keys for encrypting messages communicated between and among the mobile node, home domain, and the foreign domain," as is recited in Claim 16.

The Examiner takes the position that, "Tisdale does teach distributing encryption keys, Tisdale merely indicates in the passage cited that these keys are not transmitted in the clear but rather encrypted, see col. 9, lines 49-56, or calculated by the MET [Mobile Earth Terminal] based on received signals see col. 10, line 61 through col. 12, line 47." (See Final Office Action, pg. 3). However, there is a stark contrast between Tisdale's distributing security keys for MET validation and authorization and Applicants' Claim 16 feature of generating a registration reply "comprising one or more encryption keys for encrypting messages communicated between and among the mobile node, home domain, and the foreign domain."

Additionally, Tisdale specifically states in the cited passage that "the keys are changeable at the MET [Mobile Earth Terminal]." Here, in the present application, the home domain "generate[s] a registration reply comprising one or more encryption keys for encrypting messages communicated between and among the mobile node, home domain, and the foreign domain." Therefore, contrary to the Examiner's assertion, Tisdale does not teach such features of Claim 16 and fails to cure the deficiencies of Inoue.

Hence, Inoue and Tisdale fail to satisfy the requirements of §2142 in that the references must "teach or suggest **all** the claim limitations." (Emphasis added). Thus, for this independent reason, it is respectfully submitted that Claim 16 is not obvious in view of Inoue and Tisdale.

Now turning to Applicants' Claim 22 which depends from and further limits independent Claim 16. Applicants' Claim 22 includes a recitation of:

> . . . wherein generating a registration reply comprises encrypting at least one of the encryption keys.

The Examiner alleges that this feature is taught by Tisdale in Col. 11, lines 14-35. (See Final Office Action, pg. 9). Applicants respectfully disagree. More specifically, the cited passage of Tisdale recites the following:

> ...The method comprises the steps of requesting, by a user, to become a subscriber in a communication system, generating a first input signal by the mobile communication system, transmitting the first input signal by the mobile communication system, transmitting the first input signal from the mobile communication system to the central controller, and generating a first security key in the central controller using data encryption algorithm using the first input signal and a second input signal generated by a random number generator. In addition, the method includes the steps of generating a third input signal responsive to the first input signal confirming receipt of the first input signal by the central controller, transmitting the third input signal from the central controller to the mobile communication system responsive to the transmitting step, generating a second security key in the mobile communication system using the data encryption algorithm using the first and second input signals, and verifying by the central controller when the mobile communication system initiates a communication that the mobile communication system is authorized to utilize the communication system responsive to the comparison of first and second components of the first and second security keys

respectively. (Emphasis added).

From the above, Tisdale teaches generating a first and second security key using data encryption algorithm. Nowhere in the cited passage does Tisdale teach using the data encryption algorithm to encrypt the first and/or second security keys. Accordingly, there is no teaching or suggestion of "wherein generating a registration reply comprises encrypting at least one of the encryption keys," as is recited in Claim 22. Applicants respectfully submit that Inoue does not cure the deficiencies of Tisdale. As previously indicated by the Examiner, "the following is not taught in [Inoue]: 'comprising one or more encryption keys for encrypting messages to be communicated between and among the mobile node[,] home [domain, and the foreign domain].'" (See Final Office Action, pg. 8) (Emphasis added). Since Inoue does not teach a registration reply comprising one or more encryption keys, Inoue cannot teach, "wherein generating a registration reply comprises encrypting at least one on the encryption keys."

Additionally, the Examiner cited essentially the same passage of Tisdale (Col. 11, lines 10-35) to reject dependent Claims 24, 26, 27, and 28. (See Final Office Action, pg. 10) Applicants respectfully submit that Tisdale does not teach the features in Claims 24, 26, 27, and 28 for at least the same reasons as set forth above for Claim 22.

As such, Inoue and Tisdale fail to satisfy the requirements of §2142 in that the references must "teach or suggest **all** the claim limitations." (Emphasis added). Thus, for this independent reason, it is respectfully submitted that Claims 22, 24, 26, 27, and 28 are not obvious in view of Inoue and Tisdale.

Now turning to Applicants' Claim 23 which indirectly depends from and further limits independent Claim 16. Applicants' Claim 23 includes a recitation of:

> . . . wherein generating a registration reply comprises encrypting the encryption keys for encrypting messages to be communicated

> between the mobile node and the home domain, and between the mobile node and foreign domain.

The Examiner alleges that this feature is taught by Inoue in Col. 4., line 63 through Col. 5, line 10. (See Final Office Action, pg. 10). Applicants respectfully disagree. More specifically, the cited passage of Inoue recites the following:

> ...a registration unit for decrypting an encrypted packet received from a packet relay device and registering the current location address into the memory unit when a decrypted packet is a registration request packet containing the current location address which is transmitted from the mobile computer to the mobile computer management device, the packet relay device being provided at a border between a private address space by which the home network is managed and a global address space and relaying a packet to be exchanged between one computer connected to the private address space and another computer connected to the global address space; and a transfer unit for transferring a packet destined for the home address of the mobile computer in the home network to the current location address according to the memory unit.

From the above, Inoue teaches a registration unit for decrypting an encrypted packet to register the current location of the mobile computer or node when it is a registration request from the mobile computer. Here, in the present application, "generating a registration reply comprises encrypting the encryption keys for encrypting messages to be communicated between the mobile node and the home domain, and between the mobile node and foreign domain," as is recited in Claim 23. Applicants respectfully submit that Tisdale does not cure the deficiencies of Inoue for

at least the same reasons as set forth above for Claim 22.

Hence, Inoue and Tisdale fail to satisfy the requirements of §2142 in that the references must "teach or suggest **all** the claim limitations." (Emphasis added). Thus, for this independent reason, it is respectfully submitted that Claim 23 is not obvious in view of Inoue and Tisdale.

The PTO Cannot Establish Obviousness With Art That Teaches Away

In evaluating obviousness, it is not proper to selectively consider only part of a reference, while ignoring other parts that teach away from the invention. More specifically, as discussed in MPEP §2141.02, case law has established that:

> A prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention. *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984). (Emphasis in original).

As discussed above, Tisdale teaches using security keys to validate and authorize a MET (Mobile Earth Terminal) in its attempt to access a communication system. Here, in the present application, the home domain receives and processes the registration request "to generate a registration reply comprising one or more encryption keys for encrypting messages communicated between and among the mobile node, home domain, and the foreign domain." Accordingly, the home domain has already authenticated the mobile node by receiving and processing the registration request from the mobile node. The home domain then generates a registration reply that includes encryption keys for encrypting messages between the mobile node, home domain, and foreign domain.

Since Tisdale teaches directly away from subject matter recited in Claim 16, it is respectfully submitted that Tisdale does not factually support a *prima facie* case of obviousness

with respect to Claims 16. Accordingly, for this independent reason alone, it is respectfully submitted that Claim 16 is not obvious under §103 in view Tisdale.

The Combination Is Improper

There is yet another reason why Inoue cannot properly be modified by Tisdale so as to meet the subject matter of Applicants' Claims 16-30. As discussed in MPEP §2142, case law relating to §103 requires that:

> To establish a *prima facie* case of obviousness, . . . there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. . . . The teaching or suggestion to make the claimed combination . . . must . . . be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

As discussed in MPEP §2143.01, case law relating to §103 has also established that:

> The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). . . . Although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so". 916 F.2d at 682, 16 USPQ2d at 1432.). (Emphasis in original).

As stated previously, the Examiner has taken the position that "[i]t would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of [Inoue] a mobile communication scheme to include means to generate a reply that utilizes one or more encryption keys as taught in [Tisdale]." It is respectfully submitted that the combination of Inoue and Tisdale is improper.

More specifically, Inoue teaches a border gateway at the exit of the organization network that facilitates communication between a mobile node and a home domain in a situation where the mobile node has moved outside the organization network. (See Inoue, Fig. 2). As such, the encryption keys corresponding to the border gateway, mobile computer, and home network (via the mobile computer management device) have been established even before generating a registration reply. For example, Inoue, in Col. 9, line 37 through Col. 10, line 21 (reference numbers omitted) (emphasis added), recites the following:

> ...the mobile computer transmits a registration request packet of the mobile IP which is encrypted using a corresponding key, to the global address interface of the border gateway at the exit of the organization network using the address set at the "Border Gateway IP address....
>
> When the encrypted packet destined to itself arrives, the border gate checks its source, decrypts this packet using a key corresponding to its source (the mobile computer in this case), and checks the content of the de[crypted] packet....
>
> Then, the border gateway re-encrypts the location registration packet using a key corresponding to the mobile computer management device of the home network which is the transfer target....

> Upon receiving the relayed an re-encrypted registration request packet from the border gateway, the mobile computer management device of the home network..., de[crypts] this packet using a key corresponding to the border gateway which is its source....
>
> In addition, in order to return a reply packet (a registration success packet) corresponding to the registration request to the mobile computer, the mobile computer management device transmits the reply packet using a key corresponding to the border gateway....

From the above, contrary to the Examiner's assertion, it would not have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of [Inoue] a mobile communication scheme to include means to generate a reply that utilizes one or more encryption keys as taught in [Tisdale]. This is because Inoue, even before sending a registration reply, has already established encryption keys for encrypting data packets corresponding to the border gateway, mobile computer, and home network (via the mobile computer management device).

The current case law makes it clear that the best defense against hindsight-based obviousness analysis is the rigorous application of the requirement for a showing of a teaching or motivation to combine the prior art references.

The present §103 rejection of Claim 16 is therefore not complete, because the Examiner fails to demonstrate the motivation that is a required element of a proper *prima facie* case. Since Inoue has already established encryption keys associated the border gateway, mobile computer, and home network, a person skilled in the art would have no motivation to modify Inoue in a manner suggested by the Examiner, unless of course that person was using hindsight of Applicants' disclosure. In particular, by using Applicant's disclosure as a blueprint that gives a 20/20 view of the desired result, the Examiner has used hindsight to propose a modification to

Inoue, despite the fact that the modification runs directly contrary to the express teachings of Inoue.

Accordingly, the §103 rejection of Claim 16 is improperly based on hindsight of Applicants' disclosure, rather than on motivation properly derived from what was known before the present application. Consequently, for this independent reason alone, it is respectfully submitted that Claim 16 is not rendered obvious under §103 in view of Inoue and Tisdale.

Request For Relief

For each of the various different reasons discussed above, it is respectfully submitted that Claim 16 is not rendered obvious under §103 by the proposed combination of Inoue and Tisdale. It is therefore respectfully requested that the Board reverse the §103 rejection of Claim 16.

Claims 17-30 depends from, either directly or indirectly, and further limits Claim 16, and are believed to be allowable for at least the same reasons as Claim 16. Furthermore, Claims 22-24, 26, 27, and 28 are believed to be allowable for the additional reasons as discussed above.

II. THE §103 REJECTION OF CLAIMS 70-75

Claims 70-75 stand rejected under 35 U.S.C. §103 as obvious in view of a proposed combination of Chuah and Cheng. However, it is respectfully submitted that these claims are not obvious in view of Chuah and Cheng. As noted earlier, the PTO recognizes in MPEP §2142 that:

> The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness.

Applicants respectfully submit that Chuah and Cheng fail to establish a *prima facie* case of obviousness under §103 with respect to Claim 70, for mutually exclusive reasons that are discussed below.

The Prior Art Must Teach All Claim Limitations Under §103

As discussed in MPEP §2142, case law relating to §103 requires that:

> To establish a *prima facie* case of obviousness . . . the prior art reference (or references when combined) must teach or suggest **all** the claim limitations. . . . *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). (Emphasis added).

Applicants' Claim 70 includes a recitation of:

> ... dynamically establishing a security association between the initiator and the responder, whereby the initiator presents to the responder a registration request that includes one or more proposals.

Applicants respectfully submit that neither Chuah nor Cheng, alone or in combination, teach or suggest all the features of Claim 70. The Examiner indicated that, "the following is not taught by [Chuah]: 'dynamically establishing a security association between the initiator and the responder.'" (See Final Office Action, pg. 5). The Examiner alleges that such feature is disclosed in Col. 7, lines 9-17 of Cheng. Applicants respectfully disagrees. More specifically, the cited passage of Cheng recites the following:

> It is an object of the present invention to provide a

> technique which improves the performance of a mobile unit (MU) in a wireless LAN or mobile IP environment, particularly during hand-over. The present invention accomplishes this by reusing rather than renegotiating the security associations (SAs) corresponding to the MU once the MU is handed-over. By reusing the SAs, less time is spent negotiating SAs. Consequently, the MU can begin secure communications almost immediately upon being handed-over from one SU to [] another SU.

From the above, Cheng describes generally a method to reuse already negotiated security associations between a mobile unit and a stationary unit when the mobile unit is handed-over to another stationary unit. Here, in the present application, the initiator presents to the responder a registration request that includes one or more proposals. In this manner, the initiator may engage in a negotiation with the responder in which the entities dynamically negotiate the security association between each other. Accordingly, the security association between the initiator and responder is dynamically established. (See Present Application, pg. 25, lines 6-14). Therefore, contrary to the Examiner's assertion, Cheng does not teach such features of Claim 70 and fails to cure the deficiencies of Chuah.

Additionally, the Examiner alleges that Chuah teaches "whereby the initiator presents to the responder a registration request that includes one or more proposals" in Col. 21, lines 42-62. However, the Examiner also notes that in the cited passage, "the subscriber's service profile inherently is a registration request that includes one or more proposals." (See Final Office Action, pg. 5). Applicants respectfully disagree. More specifically, Chuah explicitly states that, "[t]he subscriber service profile is stored in a subscriber directory" (Col. 21, lines 46-51) and that, "the home registration server accesses the subscriber directory to learn detail subscriber information (e.g., quality of service options subscribed to, etc.)" (Col. 22, lines 37-40) in response to a registration request from an end system (or subscriber) located in a foreign

network. (See also Chuah, Fig. 19). Accordingly, contrary to the Examiner's assertion, Chuah's subscriber's service profile is not inherently a registration request that includes one or more proposals.

Hence, Chuah and Cheng fail to satisfy the requirements of §2142 in that the references must "teach or suggest **all** the claim limitations." (Emphasis added). Thus, for this independent reason, it is respectfully submitted that Claim 70 is not obvious under §103 in view of Chuah and Cheng.

There Is No Motivation To Modify Chuah

There is yet another reason why Chuah cannot properly be modified so as to meet the subject matter of Applicants' Claim 70. As discussed in MPEP §2142, case law relating to §103 requires that:

> To establish a *prima facie* case of obviousness, . . . there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. . . . The teaching or suggestion to make the claimed combination . . . must . . . be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Further, as discussed in MPEP §2143.01, case law has established that:

> The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916

> F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). . . . Although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so". 916 F.2d at 682, 16 USPQ2d at 1432.). (Emphasis in original).

As discussed above, the Examiner admits that Chuah does not disclose the step of "dynamically establishing a security association between the initiator and the responder." Cheng does not overcome this deficiency, because the entire thrust of Cheng is to a method of reusing already negotiated security associations between a mobile unit and a stationary unit when the mobile unit is handed-over to another stationary unit. Here, in the present application, the security association between the initiator and responder is dynamically established "whereby the initiator presents to the responder a registration request that includes one or more proposals." In this manner, the method of establishing security associations between entities is dynamic and not static, where an infinite number of predefined shared secrets or encryption keys may be required. (See Present Application, pg. 1, line 29 through pg. 2, line 3). The present §103 rejection of Claim 70 is therefore not complete, because the Examiner fails to demonstrate the motivation that is a required element of a proper *prima facie* case. Since Cheng quite literally teaches away from what is recited in Claim 70, a person skilled in the art would have no motivation to modify Chuah by using teachings from Cheng in a manner that directly contravenes the teachings of Cheng, unless of course that person was using hindsight of Applicants' disclosure.

Accordingly, the §103 rejection of Claim 70 is improperly based on hindsight of Applicants' disclosure, rather than on motivation properly derived from what was known before the present invention. Consequently, for this independent reason alone, it is respectfully submitted that Claim 70 is not rendered obvious under §103 by Chuah and Cheng.

Request For Relief

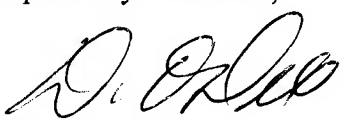
For each of the various different reasons discussed above, it is respectfully submitted that Claim 70 is not rendered obvious under §103 by the proposed combination of Chuah and Cheng. It is therefore respectfully requested that the Board reverse the §103 rejection of Claim 17.

Claims 71-75 depend from, either directly or indirectly, and further limit independent Claim 70 and thus, are allowable for at least the same reasons as Claim 70.

IX. CONCLUSION

For reasons discussed above, it is respectfully submitted that the rejections of each of pending Claims 16-30 and 70-75 are erroneous. Accordingly, it is respectfully requested that the Board reverse the claim rejections discussed in the foregoing arguments.

Respectfully submitted,



David M. O'Dell
Registration No. 42,044

Date: March 29, 2007

HAYNES AND BOONE, LLP
901 Main Street, Suite 3100
Dallas, Texas 75202-3789
Telephone: (972) 739-8636
Facsimile: (214) 200-0853
File: 22171.321 / 11349RRUS04U

Enclosures: Claims Appendix
Evidence Appendix
Related Proceedings Appendix

Certificate of Service

I hereby certify that this correspondence is being filed with the U.S. Patent and Trademark Office via EFS-Web on March 29, 2007.

Bonnie Boyle

Bonnie Boyle

R-161534.1

CLAIMS APPENDIX

16. A method of providing secure communication between a mobile node and home domain using a foreign domain, comprising:

transmitting a registration request from the mobile node to the home domain the request comprising an identity of a user of the mobile node in encrypted form and network routing information in non-encrypted form;

the home domain receiving and processing the registration request to generate a registration reply comprising one or more encryption keys for encrypting messages communicated between and among the mobile node, home domain, and the foreign domain; and

transmitting the registration reply from the home domain to the foreign domain and the mobile node.

17. The method of claim 16, wherein transmitting a registration request from the mobile node to the home domain comprises:

transmitting the registration request from the mobile node to the foreign domain; and

transmitting the registration request from the foreign domain to the home domain.

18. The method of claim 17, wherein transmitting the registration request from the foreign domain to the home domain comprises establishing a secure communication pathway between the foreign domain and the home domain.

19. The method of claim 17, wherein transmitting the registration request from the foreign domain to the home domain comprises establishing a secure communication pathway between the foreign domain and the mobile node.

20. The method of claim 17, wherein transmitting the registration request from the foreign domain to the home domain comprises establishing a secure communication pathway between the home domain and the mobile node.

21. The method of claim 16, wherein processing the registration request from the mobile node within the home domain comprises decrypting the encrypted form of the identity of the user.

22. The method of claim 16, wherein generating a registration reply comprises encrypting at least one of the encryption keys.

23. The method of claim 22, wherein generating a registration reply comprises encrypting the encryption keys for encrypting messages to be communicated between the mobile node and the home domain, and between the mobile node and the foreign domain.

24. The method of claim 22, further comprising:

decrypting one or more of the encrypted encryption keys.

25. The method of claim 16, wherein generating the registration reply comprises:

generating a first encryption key for encrypting messages to be communicated between the mobile node and the home domain;

generating a second encryption key for encrypting messages to be communicated between the foreign domain and the home domain; and

generating a third encryption key for encrypting messages to be communicated between the foreign domain and mobile node.

26. The method of claim 22, wherein generating the registration reply comprises encrypting at least one of the first and third encryption keys.

27. The method of claim 26, further comprising:

decrypting at least one of the encrypted first and third encryption keys.

28. The method of claim 16, wherein the registration reply includes:

encryption keys that are encrypted; and

encryption keys that are not encrypted.

29. The method of claim 28, further including:

extracting one or more of the encryption keys that are not encrypted from the registration reply.

30. The method of claim 28, further including:

extracting and decrypting one or more of the encryption keys that are encrypted from the registration reply.

70. A method of providing secure communications between an initiator and a responder in a communication network, comprising:

dynamically establishing a security association between the initiator and the responder, whereby the initiator presents to the responder a registration request that includes one or more proposals.

71. The method of claim 70, further comprising:

negotiating the security association.

72. The method of claim 71, wherein negotiating the security association comprises:

negotiating one or more security transforms to be used to provide secure communications between the initiator and the responder.

73. The method of claim 71, wherein negotiating the security association comprises:

proposing the number of transforms to be used to provide secure communications between the initiator and the responder.

74. The method of claim 71, wherein negotiating the security association comprises:

proposing the duration of at least a portion of the security association.

75. The method of claim 71, wherein negotiating the security association comprises:

proposing the type of transforms to be used to provide secure communications between the initiator and the responder.

EVIDENCE APPENDIX

(None).

RELATED PROCEEDINGS APPENDIX

(None).